

FQ5-511

32

## Claims:

1. A system comprising:

a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information provided by a manager subsystem; and

5 a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session,

wherein

the participant subsystem comprises:

10 an anonymous signing section for authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with anonymous signature, and

the reception subsystem comprises:

15 an anonymous signature determining section for determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem; and

20 a sender match determining section for determining whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

FOLE FQ 034/057

FQ5-511

33

2. The system according to claim 1, wherein the anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the sender  
5 match determining section checks the data included in the anonymous signature of received anonymous participation data.

3. The system according to claim 2, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the  
10 secret information.

4. The system according to claim 1, wherein the anonymous signing section authorizes the individual data based on a group signature scheme.

5. The system according to claim 1, wherein the  
15 anonymous signing section authorizes the individual data based on an escrowed identity scheme.

6. The system according to claim 1, wherein the anonymous signing section comprises:

a generator creating section for creating a  
20 session-dependent generator depending on the session-related information;

00765390-04394  
"000000"00000000

FQ5-511

34

a group signing section for signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by

5 raising the session-dependent generator to a power determined by the secret information; and

a linkage data generating section for generating linkage data indicating a relationship among the session-dependent generator and a generator determined by the

10 individual data and/or the session-related information.

7. The system according to claim 6, wherein the secret information is represented by  $(x, y, v)$  that satisfies:  $v = (y + \delta)^{1/e} \bmod n$ , where  $y = a^x \bmod n$ ,  $n$  is a product of two prime numbers as used in the RSA cryptography,  $g$  is a generator that

15 generates a cyclic group of order  $n$ ,  $a$  is an integer mutually prime to  $n$ ,  $e$  is an integer mutually prime to the Euler number of  $n$ , and  $\delta$  is a constant other than 1.

the generator creating section creates a session-dependent generator  $g_A$  corresponding to a session  $A$

20 and a generator  $g_m$  is generated based on the individual data  $m$  and/or the session  $A$ .

the group signing section sets  $z = g_A^x$  and generates a first proof statement

$$V_1 = \text{SKLOGLOG}(z, g_A, a) [\alpha: z = g_A^{(a^\alpha)}] (1)$$

FQ5-511 036/057

FQ5-511

35

proving the knowledge of  $\alpha$  satisfying  $z = g_A(\alpha)$ , and a second proof statement

$$V_2 = \text{SKROOTLOG}(z * g_A^b, g_A, e) [\beta: z * g_A^b = g_A(\beta^e)](1)$$

proving the knowledge of  $\beta$  satisfying  $z * g_A^b = g_A(\beta^e)$ ,

5 the linkage data generating section sets  $z_1 = g_m^y$ , and generates a third proof statement

$$V_3 = \text{SKREP}(z_1/z, g_m/g_A) [\gamma: z_1/z = (g_m/g_A)^\gamma](1)$$

proving the knowledge of  $z_1$  and  $z$  have the same power to the bases  $g_m$  and  $g_A$ , respectively.

10 wherein the anonymous participation data is defined as  $(A, m, z, z_1, V_1, V_2, V_3)$ .

8. The system according to claim 7, wherein

the anonymous signature determining section checks  $V_1$ ,  $V_2$ , and  $V_3$  of the anonymous participation data to determine  
15 whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks  $z$  of the anonymous participation data to determine whether anonymous  
20 signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

9. The system according to claim 1, wherein the anonymous signing section comprises:

FOLEY & LARDNER

FQ5-511

36

a generator creating section for creating a generator depending on the session-related information;

a group signing section for signing the individual data using the generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

10. The system according to claim 9, wherein the secret information is represented by  $(x, y, v)$  that satisfies:  $v = (y + \delta)^{1/e} \bmod n$ , where  $y = a^x \bmod n$ , the individual data is denoted by  $m$ ,  $n$  is a product of two prime numbers as used in the RSA cryptography,  $g$  is a generator that generates a cyclic group of order  $n$ ,  $a$  is an integer mutually prime to  $n$ ,  $e$  is an integer mutually prime to the Euler number of  $n$ , and  $\delta$  is a constant other than 1,

the generator creating section creates a session-dependent generator  $g_A$  corresponding to a session  $A$ .

the group signing section sets  $z = g_A^x$  and generates a first proof statement

$$V_1 = \text{SKLOGLOG}(z, g_A, a) [\alpha: z = g_A^{(\alpha)}] (m)$$

proving the knowledge of  $\alpha$  satisfying  $z = g_A^{(\alpha)}$ , and a second proof statement

$$V_2 = \text{SKROOTLOG}(z * g_A^{\delta}, g_A, e) [\beta: z * g_A^{\delta} = g_A^{(\beta^e)}] (m)$$

proving the knowledge of  $\beta$  satisfying  $z * g_A^{\delta} = g_A^{(\beta^e)}$ ,

FQ5-511

37

wherein the anonymous participation data 13 is designated as  $(A, m, z, V_1, V_2)$ .

11. The system according to claim 10, wherein

the anonymous signature determining section checks

5  $V_1$ , and  $V_2$  of the anonymous participation data to determine whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

10 the sender match determining section checks  $z$  of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

12. The system according to claim 1, wherein the anonymous signing section comprises:

15 a generator creating section for creating a session-dependent generator depending on the session-related information;

an escrow identifying section for signing the individual data using the session-dependent generator and the  
20 secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

0075599-01224

38

13. The system according to claim 12, wherein the secret information is represented by  $(a, b)$  that satisfies  $b = (a^e - \delta)^{1/e} \bmod n$ , where  $n$  is a product of two prime numbers as used in the RSA cryptography,  $g$  is a generator that generates a cyclic group of order  $n$ ,  $a$  is an integer mutually prime to  $n$ ,  $e$  is an integer mutually prime to the Euler number of  $n$ , and  $\delta$  is a constant other than 1.

the escrow identifying section sets  $x_a = g_A(x^a)$  and generates a first proof statement

proving the knowledge of  $\alpha$  satisfying  $x_a = g_\alpha(a^a)$ , and sets  $x_b = g_\alpha(b^a)$  and generates a second proof statement

proving the knowledge of  $\beta$  satisfying  $z_b = g_A(b^d)$ , and

$$V_1 = \text{SKREP}(z_c/z_n, g_m/g_A)[\gamma: z_c/z_n = (g_m/g_A)^\gamma] \quad (1)$$

FQ5-511

39

proving the knowledge of  $z_a$  and  $z_b$  having the same power to the bases  $g_a$  and  $g_b$ , respectively,

wherein the anonymous participation data is defined as  $(A, m, z_a, z_b, z_o, V_1, V_2, V_3)$ .

5           14. The system according to claim 13, wherein  
the anonymous signature determining section  
determines whether  $z_a/z_b = g_a^s$  is satisfied and checks  $V_1$ ,  $V_2$ ,  
and  $V_3$  of the anonymous participation data to determine whether  
received data is anonymous participation data with anonymous  
10 signature authorized by the participant subsystem, and

the sender match determining section checks one of  
 $z_a$  and  $z_b$  of the anonymous participation data to determine  
whether anonymous signatures of arbitrary two pieces of  
anonymous participation data are signed by an identical  
15 participant subsystem.

15. The system according to claim 1, wherein the  
anonymous signing section comprises:

a generator creating section for creating a  
session-dependent generator depending on the session-related  
20 information; and

an escrow identifying section for signing the  
individual data using the session-dependent generator and the  
secret information to produce anonymous participation data,  
wherein the anonymous participation data includes data

FOLETO-06E99260



40

16. The system according to claim 15, wherein the secret information is represented by  $(a, b)$  that satisfies

the generator creating section creates a session-dependent generator  $g_i$  corresponding to a session  $A$ ,

$$V_1 = \text{SKROOTLOG}(z_1, g_1, e) [\alpha: z_1 = g_1(g^{\alpha})] (m)$$
$$V_2 = \text{SKROOTLOG}(z_b, g_A, e) [\beta: z_b = g_A(b^e)](m)$$

wherein the anonymous participation data is defined

17. The system according to claim 16, wherein

the anonymous signature determining section determines whether  $z_a/z_h = g_a^b$  is satisfied and checks  $V_1$  and  $V_2$  of the anonymous participation data to determine whether

FQ5-511

41

received data is anonymous participation data with anonymous signature authorized by the participant subsystem, and

the sender match determining section checks one of  $z_s$  and  $z_r$  of the anonymous participation data to determine whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

18. An anonymous participation authority management method for a system comprising:

10 a participant subsystem that is authorized to anonymously participate in a plurality of sessions using secret information; and

a reception subsystem that determines whether it is acceptable for the participant subsystem to participate in a session.

the method comprising the steps of:

at the participant subsystem,

a) authorizing individual data using the secret information depending on session-related information to produce anonymous participation data with anonymous signature;

at the reception subsystem,

b) determining whether received data is anonymous participation data with anonymous signature authorized by the participant subsystem; and

FOLE F0029260

FQ5-511

42

c) determining whether anonymous signatures of arbitrary two pieces of anonymous participation data are signed by an identical participant subsystem.

19. The method according to claim 18, wherein the  
5 anonymous signature includes data that is generated by a predetermined expression using the session-related information and the secret information, wherein the step (c) is performed by checking the data included in the anonymous signature of received anonymous participation data.

10 20. The method according to claim 19, wherein the predetermined expression is represented by raising a session-dependent base to a power that is dependent on the secret information.

21. The method according to claim 18, wherein the step  
15 (a) comprises the steps of:

creating a session-dependent generator depending on the session-related information;

signing the individual data using the session-dependent generator and the secret information to produce  
20 anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information; and

F022F0:05E3260

43

22. The method according to claim 18, wherein the step (a) comprises the steps of:

signing the individual data using the session-dependent generator and the secret information to produce anonymous participation data, wherein the anonymous participation data includes data obtained by raising the session-dependent generator to a power determined by the secret information.

1. *Chlorophyll a* (Chl *a*)  
 2. *Chlorophyll b* (Chl *b*)  
 3. *Chlorophyll c* (Chl *c*)  
 4. *Chlorophyll d* (Chl *d*)  
 5. *Chlorophyll e* (Chl *e*)  
 6. *Chlorophyll f* (Chl *f*)  
 7. *Chlorophyll g* (Chl *g*)  
 8. *Chlorophyll h* (Chl *h*)  
 9. *Chlorophyll i* (Chl *i*)  
 10. *Chlorophyll j* (Chl *j*)  
 11. *Chlorophyll k* (Chl *k*)  
 12. *Chlorophyll l* (Chl *l*)  
 13. *Chlorophyll m* (Chl *m*)  
 14. *Chlorophyll n* (Chl *n*)  
 15. *Chlorophyll o* (Chl *o*)  
 16. *Chlorophyll p* (Chl *p*)  
 17. *Chlorophyll q* (Chl *q*)  
 18. *Chlorophyll r* (Chl *r*)  
 19. *Chlorophyll s* (Chl *s*)  
 20. *Chlorophyll t* (Chl *t*)  
 21. *Chlorophyll u* (Chl *u*)  
 22. *Chlorophyll v* (Chl *v*)  
 23. *Chlorophyll w* (Chl *w*)  
 24. *Chlorophyll x* (Chl *x*)  
 25. *Chlorophyll y* (Chl *y*)  
 26. *Chlorophyll z* (Chl *z*)  
 27. *Chlorophyll aa* (Chl *aa*)  
 28. *Chlorophyll ab* (Chl *ab*)  
 29. *Chlorophyll ac* (Chl *ac*)  
 30. *Chlorophyll ad* (Chl *ad*)  
 31. *Chlorophyll ae* (Chl *ae*)  
 32. *Chlorophyll af* (Chl *af*)  
 33. *Chlorophyll ag* (Chl *ag*)  
 34. *Chlorophyll ah* (Chl *ah*)  
 35. *Chlorophyll ai* (Chl *ai*)  
 36. *Chlorophyll aj* (Chl *aj*)  
 37. *Chlorophyll ak* (Chl *ak*)  
 38. *Chlorophyll al* (Chl *al*)  
 39. *Chlorophyll am* (Chl *am*)  
 40. *Chlorophyll an* (Chl *an*)  
 41. *Chlorophyll ao* (Chl *ao*)  
 42. *Chlorophyll ap* (Chl *ap*)  
 43. *Chlorophyll aq* (Chl *aq*)  
 44. *Chlorophyll ar* (Chl *ar*)  
 45. *Chlorophyll as* (Chl *as*)  
 46. *Chlorophyll at* (Chl *at*)  
 47. *Chlorophyll au* (Chl *au*)  
 48. *Chlorophyll av* (Chl *av*)  
 49. *Chlorophyll aw* (Chl *aw*)  
 50. *Chlorophyll ax* (Chl *ax*)  
 51. *Chlorophyll ay* (Chl *ay*)  
 52. *Chlorophyll az* (Chl *az*)  
 53. *Chlorophyll aza* (Chl *aza*)  
 54. *Chlorophyll abz* (Chl *abz*)  
 55. *Chlorophyll acz* (Chl *acz*)  
 56. *Chlorophyll adz* (Chl *adz*)  
 57. *Chlorophyll aez* (Chl *aez*)  
 58. *Chlorophyll afz* (Chl *afz*)  
 59. *Chlorophyll agz* (Chl *agz*)  
 60. *Chlorophyll ahz* (Chl *ahz*)  
 61. *Chlorophyll aiz* (Chl *aiz*)  
 62. *Chlorophyll ajz* (Chl *ajz*)  
 63. *Chlorophyll akz* (Chl *akz*)  
 64. *Chlorophyll alz* (Chl *alz*)  
 65. *Chlorophyll amz* (Chl *amz*)  
 66. *Chlorophyll anz* (Chl *anz*)  
 67. *Chlorophyll aoz* (Chl *aoz*)  
 68. *Chlorophyll apz* (Chl *apz*)  
 69. *Chlorophyll aqz* (Chl *aqz*)  
 70. *Chlorophyll arz* (Chl *arz*)  
 71. *Chlorophyll asz* (Chl *asz*)  
 72. *Chlorophyll atz* (Chl *atz*)  
 73. *Chlorophyll auz* (Chl *auz*)  
 74. *Chlorophyll avz* (Chl *avz*)  
 75. *Chlorophyll awz* (Chl *awz*)  
 76. *Chlorophyll axz* (Chl *axz*)  
 77. *Chlorophyll ayz* (Chl *ayz*)  
 78. *Chlorophyll ayz* (Chl *ayz*)  
 79. *Chlorophyll azz* (Chl *azz*)  
 80. *Chlorophyll azaa* (Chl *aza*)  
 81. *Chlorophyll abz* (Chl *abz*)  
 82. *Chlorophyll acz* (Chl *acz*)  
 83. *Chlorophyll adz* (Chl *adz*)  
 84. *Chlorophyll aez* (Chl *aez*)  
 85. *Chlorophyll afz* (Chl *afz*)  
 86. *Chlorophyll agz* (Chl *agz*)  
 87. *Chlorophyll ahz* (Chl *ahz*)  
 88. *Chlorophyll aiz* (Chl *aiz*)  
 89. *Chlorophyll ajz* (Chl *ajz*)  
 90. *Chlorophyll akz* (Chl *akz*)  
 91. *Chlorophyll alz* (Chl *alz*)  
 92. *Chlorophyll amz* (Chl *amz*)  
 93. *Chlorophyll anz* (Chl *anz*)  
 94. *Chlorophyll aoz* (Chl *aoz*)  
 95. *Chlorophyll apz* (Chl *apz*)  
 96. *Chlorophyll aqz* (Chl *aqz*)  
 97. *Chlorophyll arz* (Chl *arz*)  
 98. *Chlorophyll asz* (Chl *asz*)  
 99. *Chlorophyll atz* (Chl *atz*)  
 100. *Chlorophyll auz* (Chl *auz*)  
 101. *Chlorophyll avz* (Chl *avz*)  
 102. *Chlorophyll awz* (Chl *awz*)  
 103. *Chlorophyll axz* (Chl *axz*)  
 104. *Chlorophyll ayz* (Chl *ayz*)  
 105. *Chlorophyll ayz* (Chl *ayz*)  
 106. *Chlorophyll ayz* (Chl *ayz*)  
 107. *Chlorophyll ayz* (Chl *ayz*)  
 108. *Chlorophyll ayz* (Chl *ayz*)  
 109. *Chlorophyll ayz* (Chl *ayz*)  
 110. *Chlorophyll ayz* (Chl *ayz*)  
 111. *Chlorophyll ayz* (Chl *ayz*)  
 112. *Chlorophyll ayz* (Chl *ayz*)  
 113. *Chlorophyll ayz* (Chl *ayz*)  
 114. *Chlorophyll ayz* (Chl *ayz*)  
 115. *Chlorophyll ayz* (Chl *ayz*)  
 116. *Chlorophyll ayz* (Chl *ayz*)  
 117. *Chlorophyll ayz* (Chl *ayz*)  
 118. *Chlorophyll ayz* (Chl *ayz*)  
 119. *Chlorophyll ayz* (Chl *ayz*)  
 120. *Chlorophyll ayz* (Chl *ayz*)  
 121. *Chlorophyll ayz* (Chl *ayz*)  
 122. *Chlorophyll ayz* (Chl *ayz*)  
 123. *Chlorophyll ayz* (Chl *ayz*)  
 124. *Chlorophyll ayz* (Chl *ayz*)  
 125. *Chlorophyll ayz* (Chl *ayz*)  
 126. *Chlorophyll ayz* (Chl *ayz*)  
 127. *Chlorophyll ayz* (Chl *ayz*)  
 128. *Chlorophyll ayz* (Chl *ayz*)  
 129. *Chlorophyll ayz* (Chl *ayz*)  
 130. *Chlorophyll ayz* (Chl *ayz*)  
 131. *Chlorophyll ayz* (Chl *ayz*)  
 132. *Chlorophyll ayz* (Chl *ayz*